ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

การวิเคราะห์มัลแวร์และการลดภัยคุกคาม คู่มือ

โทรจัน แรนซัมแวร์ สปายแวร์ รูทคิต แซนด์บ็อกซ์เสมือน การกักกัน

ภาพรวมการเรียนรู้การวิเคราะห์มัลแวร์

ได้รับการรักษาความปลอดภัย

การเข้ารหัสข้อมูล

มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด

มาตรฐานสากล

กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์

นโยบายการเข้าถึง

การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการวิเคราะห์และป้องกันมัลแวร์ คุณจะได้สำรวจสปายแวร์ โทรจัน เพย์โหลดแรนซัมแวร์ เครื่องมือวิศวกรรมย้อนกลับ พฤติกรรมของรูทคิท และกลยุทธ์การจำกัดความเสียหาย

จุดตรวจสอบของใบงาน

- ☐ **ส่วนที่ 1-4: เรียนรู้ความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามให้เชี่ยวชาญ**
- ☐ **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- ☐ **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- ☐ **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- ☐ **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- ☐ **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความปลอดภัยไซเบอร์ของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/malware/

เส้นทางการเรียนรู้การลดผลกระทบจากมัลแวร์ของคุณ

- จำแนกความแตกต่างระหว่างมัลแวร์ประเภทโทรจัน เวิร์ม และรูทคิท
- ใช้การรันแบบเวอร์ชวลไลเซชันแซนด์บ็อกซ์สำหรับวิเคราะห์โค้ด
- ออกแบบแผนการกักกันและการทำความสะอาดสำหรับเพย์โหลดแรนซัมแวร์ที่กำลังทำงาน

คำแนะนำคู่มือการวิเคราะห์มัลแวร์

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การลดผลกระทบจากมัลแวร์ ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การวิเคราะห์มัลแวร์และการควบคุมภัยคุกคาม (บทนำ)

โค้ดอันตราย เช่น โทรจัน เวิร์ม และแรนซัมแวร์ เป็นภัยคุกคามที่มีผลกระทบสูงต่อเอ็นด์พอยต์และเซิร์ฟเวอร์ ทีมรักษาความปลอดภัยวิเคราะห์มัลแวร์ในแซนด์บ็อกซ์เสมือน และใช้มาตรการแยกเครือข่ายอย่างรวดเร็วเพื่อควบคุมการแพร่กระจายของเพย์โหลด

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. ลักษณะเฉพาะที่กำหนดม้าโทรจันคืออะไร?
   - A. ปลอมตัวเป็นซอฟต์แวร์ที่ถูกต้องเพื่อหลอกให้ผู้ใช้รัน
   - B. ทำสำเนาตัวเองอัตโนมัติผ่านสายเครือข่ายภายใน
   - C. ติดไฟล์ภายในแซนด์บ็อกซ์เสมือนที่แยกต่างหาก
   - D. ดักทราฟฟิกของผู้ให้บริการอินเทอร์เน็ต

2. มัลแวร์ประเภทใดที่เข้ารหัสไฟล์และเรียกเก็บเงิน?
   - A. แรนซัมแวร์
   - B. สปายแวร์
   - C. รูทคิต
   - D. แอดแวร์

3. อะไรแสดงถึงสปายแวร์?
   - A. มัลแวร์ที่ออกแบบมาเพื่อแอบตรวจสอบการกดแป้นพิมพ์และกิจกรรมเบราว์เซอร์ของผู้ใช้
   - B. โค้ดโปรแกรมที่ทำงานภายในคอนเทนเนอร์เสมือนแบบแซนด์บ็อกซ์
   - C. การอัปเดตแอนตี้มัลแวร์ที่ดาวน์โหลดจากรีจิสทรีฐานข้อมูล
   - D. การปรับความสว่างหน้าจออัตโนมัติ

4. เหตุใดนักพัฒนามัลแวร์จึงใช้รูทคิท?
   - A. เพื่อซ่อนโพรเซสที่ทำงานอยู่และไฟล์อันตรายจากระบบปฏิบัติการ
   - B. เพื่อเพิ่มความเร็วในการประมวลผลของ CPU บนอุปกรณ์ปลายทาง
   - C. เพื่อสำรองไฟล์ฐานข้อมูลไปยังห้องนิรภัยบนคลาวด์ที่ปลอดภัย
   - D. เพื่อยืดอายุแบตเตอรี่บนแล็ปท็อป

5. แซนด์บ็อกซ์หมายถึงอะไรในการวิเคราะห์มัลแวร์?
   - A. การรันไฟล์น่าสงสัยในห้องนิรภัยเสมือนที่แยกต่างหากเพื่อสังเกตพฤติกรรมอย่างปลอดภัย
   - B. การสแกนแฮชของไฟล์กับฐานข้อมูลภัยคุกคามที่รู้จัก
   - C. กู้คืนข้อมูลสำรองของฐานข้อมูลหลังการบุกรุก
   - D. การตัดการเชื่อมต่อเราเตอร์เครือข่ายภายในจากสายสาธารณะ

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. เวิร์มคอมพิวเตอร์ต้องอาศัยการโต้ตอบของผู้ใช้จึงจะแพร่กระจายผ่านเครือข่ายภายในได้

- ○ จริง
- ○ เท็จ

7 คำถาม 7

7. แอดแวร์ไม่เป็นอันตรายเสมอและไม่ติดตามพฤติกรรมผู้ใช้หรือประวัติเบราว์เซอร์

- ○ จริง
- ○ เท็จ

8 คำถาม 8

8. การกู้คืนข้อมูลสำรองออฟไลน์ที่สะอาดช่วยให้เหยื่อกู้ไฟล์ที่ถูกเข้ารหัสได้โดยไม่ต้องจ่ายค่าไถ่

- ○ จริง
- ○ เท็จ

9 คำถาม 9

9. แอนติไวรัสแบบอิงซิกเนเจอร์หยุดมัลแวร์ zero-day ได้อย่างน่าเชื่อถือก่อนที่จะมีซิกเนเจอร์ของมัน

- ○ จริง
- ○ เท็จ

10 คำถาม 10

10. มัลแวร์ไร้ไฟล์รันสคริปต์อันตรายในหน่วยความจำของระบบ หลีกเลี่ยงการเขียนไฟล์ลงดิสก์

- ○ จริง
- ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. มัลแวร์ที่ปลอมเป็นโปรแกรมอรรถประโยชน์ที่ปลอดภัยคือ _____
2. เพย์โหลดประสงค์ร้ายที่ล็อกระบบฐานข้อมูลเพื่อเรียกเงินคือ _____
3. คีย์ล็อกเกอร์ที่แอบบันทึกรหัสผ่านคือ _____
4. การซ่อนตัวลึกในเคอร์เนลของระบบปฏิบัติการต้องใช้ _____
5. การวิเคราะห์ไฟล์น่าสงสัยในห้องนิรภัยที่แยกขาดใช้ _____ เสมือน
6. การหยุดการแพร่ของเพย์โหลดมัลแวร์ที่ทำงานอยู่ต้องมีการ _____ เครือข่ายทันที

คลังคำศัพท์

กักกัน แซนด์บ็อกซ์ โทรจัน รูทคิต แรนซัมแวร์ ไร้ไฟล์ เวิร์ม สปายแวร์

เขียนคำตอบของคุณที่นี่:

1.
2.
3.
4.
5.
6.

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

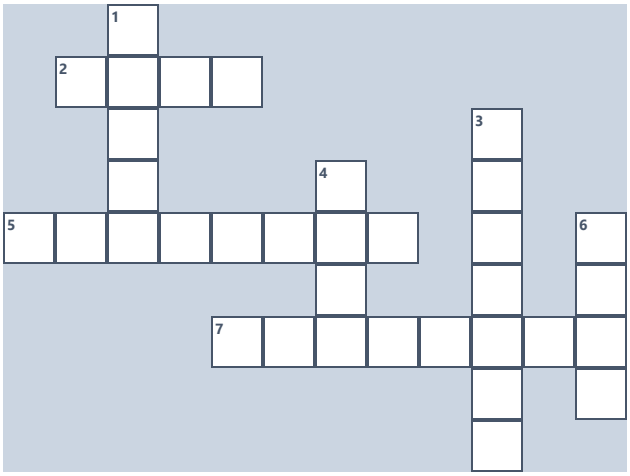
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. โทรจัน**	**A**	โปรแกรมที่ออกแบบมาเพื่อแอบเฝ้าดูและบันทึกกิจกรรมและข้อมูลที่ผู้ใช้ป้อน
☐	**2. แรนซัมแวร์**	**B**	มัลแวร์ที่ทำงานโดยตรงใน RAM เพื่อหลบการตรวจจับของตัวสแกนดิสก์
☐	**3. สปายแวร์**	**C**	การจำกัดอุปกรณ์ปลายทางที่ติดเชื้อเพื่อป้องกันการแพร่กระจายของเพย์โหลดภัยคุกคาม
☐	**4. รูทคิต**	**D**	ซอฟต์แวร์อันตรายที่ปลอมตัวเป็นโปรแกรมอรรถประโยชน์ที่ไม่เป็นอันตรายหรือมีประโยชน์
☐	**5. แซนด์บ็อกซ์**	**E**	มัลแวร์ที่แพร่กระจายตัวเองข้ามเครือข่ายโดยไม่ต้องมีการกระทำของมนุษย์
☐	**6. การจำกัดขอบเขต**	**F**	มัลแวร์ที่เข้ารหัสที่เก็บข้อมูลของระบบและเรียกร้องเงินเพื่อส่งมอบคีย์
☐	**7. เวิร์ม**	**G**	สภาพแวดล้อมเสมือนแบบแยกส่วนที่ใช้วิเคราะห์ไฟล์อันตรายอย่างปลอดภัย
☐	**8. ไร้ไฟล์**	**H**	มัลแวร์ซ่อนตัวที่ซ่อนลึกในเคอร์เนลของระบบเพื่อรักษาการควบคุมระดับผู้ดูแล

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. มัลแวร์แฝงตัวลึกในเคอร์เนลของระบบเพื่อรักษาการควบคุมระดับผู้ดูแลไว้ (4)

5. สภาพแวดล้อมเสมือนที่แยกขาดซึ่งใช้วิเคราะห์ไฟล์อันตรายอย่างปลอดภัย (8)

7. มัลแวร์ที่เข้ารหัสพื้นที่จัดเก็บของระบบและเรียกค่าไถ่เพื่อส่งมอบกุญแจ (8)

แนวตั้ง

1. ซอฟต์แวร์ประสงค์ร้ายที่ปลอมตัวเป็นโปรแกรมอรรถประโยชน์ที่ไม่เป็นอันตรายหรือมีประโยชน์ (5)

3. โปรแกรมที่ออกแบบมาเพื่อแอบเฝ้าดูและบันทึกกิจกรรมและข้อมูลที่ผู้ใช้ป้อน (7)

4. การจำกัดอุปกรณ์ปลายทางที่ติดเชื้อเพื่อป้องกันการแพร่ของเพย์โหลดภัยคุกคาม (4)

6. มัลแวร์ที่ทำสำเนาตัวเองและแพร่ผ่านเครือข่ายโดยไม่ต้องมีการกระทำของมนุษย์ (4)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: มัลแวร์แฝงตัวลึกในเคอร์เนลของระบบเพื่อรักษาการควบคุมระดับผู้ดูแลไว้ (4 ตัวอักษร):

5 แนวนอน: สภาพแวดล้อมเสมือนที่แยกขาดซึ่งใช้วิเคราะห์ไฟล์อันตรายอย่างปลอดภัย (8 ตัวอักษร):

7 แนวนอน: มัลแวร์ที่เข้ารหัสพื้นที่จัดเก็บของระบบและเรียกค่าไถ่เพื่อส่งมอบกุญแจ (8 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: ซอฟต์แวร์ประสงค์ร้ายที่ปลอมตัวเป็นโปรแกรมอรรถประโยชน์ที่ไม่เป็นอันตรายหรือมีประโยชน์ (5 ตัวอักษร):

3 แนวตั้ง: โปรแกรมที่ออกแบบมาเพื่อแอบเฝ้าดูและบันทึกกิจกรรมและข้อมูลที่ผู้ใช้ป้อน (7 ตัวอักษร):

4 แนวตั้ง: การจำกัดอุปกรณ์ปลายทางที่ติดเชื้อเพื่อป้องกันการแพร่ของเพย์โหลดภัยคุกคาม (4 ตัวอักษร):

6 แนวตั้ง: มัลแวร์ที่ทำสำเนาตัวเองและแพร่ผ่านเครือข่ายโดยไม่ต้องมีการกระทำของมนุษย์ (4 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ก	ก	ก	ต	ต	ค	ก	ผ	น	า	า	ร	า	ก	ด
ส	ก	ส	ต	า	า	ต	พ	ส	จ	ส	า	ท	น	ว
บ	ต	ส	ว	จ	ท	ล	ท	ด	า	ร	ก	ต	ค	ท
า	า	า	ร	อ	ส	ฟ	ก	า	ร	ส	ท	พ	น	ต
ส	า	ก	ผ	ส	ช	ล์	บ	ร	ฟ	ต	ด	โ	า	ด
แ	ด	เ	า	พ	ฟ	า	ค	า	ม	ช	ร	ส	ว	ว
ร	ด	า	ว	ไ	บ	บ	ส	ด	ย	า	ช	ด	ก	ห
น	ม	ฟ	ร้	ร์	น	ม	ง	ด	ร	ส	ช	ม	ก	า
ช้	า	ไ	ส	ต	ม	ม	ส	ป	า	ย	แ	ว	ร์	ค
ม	ผ	ซ์	ก	อ	บ	ด์	น	ช	แ	บ	ด	ม	ก	ท
แ	ช	ผ	ง	ต	ย	า	ก	พ	ว	ห	ท	ร	ท	ร
ว	ต	า	ค	น	น	กั	ต	า	น	ต	ด	ข	ท	ก
ร์	ผ	ด	า	ร	ก	ผ	ง	ด	ส	ว	ก	ง	ง	ห
ส	ด	ร	ต	กั	า	ม	ส	ส	า	ต	พ	ร	า	า
น	า	พ	น	ล	ล	ม	า	ป	น	ม	า	ข	ด	ฟ

รายการคำศัพท์

โทรจัน แรนซัมแวร์ สปายแวร์ รูทคิต แซนด์บอกซ์ กักกัน เวิร์ม ไร้ไฟล์

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ

A. โทรจัน

B. แรนซัมแวร์

C. สปายแวร์

D. รูทคิต

E. แซนด์บอกซ์

F. กักกัน

G. เวิร์ม

H. ไร้ไฟล์

คำนิยามและช่องจับคู่

1. มัลแวร์แฝงตัวลึกในเคอร์เนลของระบบเพื่อรักษาการควบคุมระดับผู้ดูแลไว้
2. การจำกัดอุปกรณ์ปลายทางที่ติดเชื้อเพื่อป้องกันการแพร่ของเพย์โหลดภัยคุกคาม
3. มัลแวร์ที่ทำงานโดยตรงใน RAM เพื่อหลบการตรวจจับของตัวสแกนดิสก์
4. มัลแวร์ที่ทำสำเนาตัวเองและแพร่ผ่านเครือข่ายโดยไม่ต้องมีการกระทำของมนุษย์
5. มัลแวร์ที่เข้ารหัสพื้นที่จัดเก็บของระบบและเรียกค่าไถ่เพื่อส่งมอบกุญแจ
6. โปรแกรมที่ออกแบบมาเพื่อแอบเฝ้าดูและบันทึกกิจกรรมและข้อมูลที่ผู้ใช้ป้อน
7. ซอฟต์แวร์ประสงค์ร้ายที่ปลอมตัวเป็นโปรแกรมอรรถประโยชน์ที่ไม่เป็นอันตรายหรือมีประโยชน์
8. สภาพแวดล้อมเสมือนที่แยกขาดซึ่งใช้วิเคราะห์ไฟล์อันตรายอย่างปลอดภัย

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. จ ร โ น ท _____
2. ส า ร์ ว แ ย ป _____
3. ด์ ซ แ บ อ ซ์ ก น _____
4. ม ร์ เ ว _____
5. ม แ ร ร์ ซ์ แ ว น _____
6. ค ิ ต ร ู ท _____
7. ก ั ก ั น ก _____
8. ส์ ไ ไ ฟ ร้ _____

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	สถานที่ดาวน์โหลดแอปที่ปลอดภัย			
2	อุปกรณ์ที่ถูกแฮกได้			
3	สิ่งที่คุณสำรองข้อมูล			
4	สัญญาณเตือนในอีเมล			
5	สัญญาณที่บ่งบอกว่าโทรศัพท์มีมัลแวร์			
6	ประเภทของมัลแวร์ที่คุณรู้จัก			
7	ประเภทไฟล์ที่ควรระวัง			
8	วิธีที่มัลแวร์เข้าสู่พีซี			
9	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
10	คำที่เกี่ยวข้องกับความปลอดภัยไซเบอร์			
11	สิ่งที่ควรทำหลังข้อมูลรั่วไหล			
12	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
13	สัตว์หรือตัวละครที่มีชื่อคล้ายมัลแวร์			
14	สิ่งที่มัลแวร์ขโมยได้			
15	สิ่งที่ควรทำหากคุณคลิกลิงก์ผิด			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การจำกัดเพย์โหลดแรนซัมแวร์ในองค์กร



สถานการณ์: เครือข่ายท้องถิ่นขององค์กรถูกแรนซัมแวร์ที่กำลังทำงานอยู่เจาะเข้ามา เซิร์ฟเวอร์ไฟล์สำคัญเริ่มแสดงนามสกุลไฟล์ .locked กำหนดนโยบายการควบคุมสถานการณ์

คำถามอภิปราย: จงอธิบายขั้นตอนการจำกัดวงโดยละเอียด และสรุปโปรโตคอลการกู้คืนข้อมูล

กรณีศึกษาที่ 2: การฉีดหน่วยความจำของมัลแวร์ไร้ไฟล์



สถานการณ์: นักวิเคราะห์ตรวจพบรูปแบบสคริปต์น่าสงสัยที่ทำงานโดยตรงใน RAM ของระบบโดยใช้เครื่องมือผู้ดูแลระบบมาตรฐาน แต่ไม่มีไฟล์อันตรายอยู่บนดิสก์

คำถามอภิปราย: จงอธิบายกลยุทธ์การวิเคราะห์หน่วยความจำ และระบุเครื่องมือเพื่อบล็อกการทำงานแบบไม่มีไฟล์ (fileless)

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ปกป้องทรัพย์สินเครือข่ายจากผู้ก่อภัยคุกคามออนไลน์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ั=48
า=49 ำ=50 ิ=51 ี=52 ึ=53 ื=54 ุ=55 ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ็=62 ่=63 ้=64 ๊=65 ๋=66 ์=67

21	35	39	8	8	48	26		57	30	34	67	59	43	37	20

27	37	49	34	23	49	7		20	64	39	34

21	48	39	57	29	64	49	20	56

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: มัลแวร์คืออะไร?

ซอฟต์แวร์อันตรายที่ผู้ไม่หวังดีออกแบบมาเพื่อทำลาย ยึดควบคุม หรือขโมยข้อมูลจากอุปกรณ์และเครือข่าย

Q2: ไวรัสกับเวิร์มต่างกันอย่างไร?

ไวรัสต้องอาศัยการกระทำของมนุษย์ (เช่น การเปิดไฟล์) จึงจะแพร่กระจาย ส่วนเวิร์มแพร่กระจายข้ามเครือข่ายโดยอัตโนมัติ

Q3: ม้าโทรจันติดเชื้อคอมพิวเตอร์ได้อย่างไร?

หลอกผู้ใช้โดยปลอมตัวเป็นโปรแกรมไม่เป็นอันตรายหรือปลอดภัย ซ่อนเพย์โหลดอันตรายไว้ข้างใน

Q4: แรนซัมแวร์คืออะไร?

มัลแวร์ประเภทหนึ่งที่เข้ารหัสไฟล์บนระบบเป้าหมายและเรียกค่าไถ่เพื่อแลกกับคีย์ถอดรหัส [1]

Q5: สปายแวร์คืออะไร?

ซอฟต์แวร์อันตรายที่แอบบันทึกการกดแป้นพิมพ์ รหัสผ่าน และพฤติกรรมการท่องเว็บของผู้ใช้เพื่อส่งให้ผู้โจมตี

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: แซนด์บ็อกซ์ (sandboxing) หมายความว่าอะไร?

การรันไฟล์ที่น่าสงสัยในสภาพแวดล้อมเสมือนที่แยกและปลอดภัยเพื่อสังเกตพฤติกรรมโดยไม่เสี่ยงต่อระบบที่ใช้งานจริง

Q7: มัลแวร์ไร้ไฟล์ (fileless malware) คืออะไร?

มัลแวร์ที่ทำงานโดยตรงในหน่วยความจำของระบบ (RAM) โดยใช้ยูทิลิตีที่ถูกต้องตามกฎ โดยไม่เขียนไฟล์ลงดิสก์เพื่อหลบตัวสแกนพื้นฐาน

Q8: รูทคิต (rootkit) ปกป้องมัลแวร์ได้อย่างไร?

ซ่อนโปรเซสและไฟล์อันตราย มักทำโดยบ่อนทำลายเคอร์เนลของระบบปฏิบัติการ ดังนั้นเครื่องสแกนแอนตี้ไวรัสอาจมองไม่เห็น

Q9: การเฝ้าติดตามพฤติกรรมแบบไดนามิกคืออะไร?

การสแกนของแอนตี้ไวรัสที่เฝ้าดูกระบวนการที่กำลังทำงานแบบเรียลไทม์ เพื่อบล็อกการกระทำที่พบได้ในมัลแวร์ เช่น การเข้ารหัสไฟล์จำนวนมาก

Q10: ทำไมการควบคุมความเสียหายจึงเร่งด่วนระหว่างการตอบสนองต่อเหตุการณ์?

การแยกปลายทางที่ถูกบุกรุกช่วยป้องกันไม่ให้เพย์โหลดมัลแวร์ที่ทำงานอยู่แพร่กระจายไปยังอุปกรณ์เครือข่ายอื่น

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: นักพัฒนามัลแวร์หลบเครื่องสแกนแอนติไวรัสที่ใช้ลายเซ็นได้อย่างไร?

ใช้พหุรูป (polymorphism) เปลี่ยนแฮชและโครงสร้างโค้ดของไฟล์ในทุกการติดเชื้อ โดยพฤติกรรมอันตรายยังคงเหมือนเดิม

Q2: ความเสี่ยงของเครื่องมือที่ใช้ได้สองทางในแคมเปญมัลแวร์คืออะไร?

ผู้โจมตีใช้เครื่องมือผู้ดูแลระบบที่ถูกกฎหมาย (เช่น PowerShell หรือ Sysinternals) เพื่อกลมกลืนกับทราฟฟิกเครือข่ายปกติ ทำให้ตรวจจับได้ยาก

Q3: process hollowing รันเพย์โหลดที่เป็นอันตรายได้อย่างไร?

เปิดโปรเซสระบบที่ถูกต้องในสถานะระงับ แทนที่โค้ดในหน่วยความจำด้วยมัลแวร์ แล้วทำงานต่อ

Q4: เซิร์ฟเวอร์ Command and Control (C2) มีบทบาทอะไร?

เซิร์ฟเวอร์ระยะไกลที่แฮกเกอร์ใช้ส่งคำสั่งและเพย์โหลดไปยังมัลแวร์ที่ทำงานบนเครื่องที่ถูกเจาะ

Q5: ทำไมการดักจับการกดแป้นพิมพ์ (keylogging) จึงตรวจจับได้ยาก?

คีย์ล็อกเกอร์พื้นฐานใช้ทรัพยากร CPU น้อยมากและซ่อนกระบวนการของตนไว้ภายในยูทิลิตีของผู้ใช้ที่ถูกกฎหมาย

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การพรางโค้ด (code obfuscation) หน่วงการวิเคราะห์มัลแวร์อย่างไร?

เข้ารหัสหรือจัดเรียงซอร์สโค้ดใหม่ ทำให้เครื่องมือของนักวิเคราะห์และเครื่องสแกนความปลอดภัยอ่านไม่ได้

Q7: บูตคิต (bootkit) ทำหน้าที่อะไร?

รูทคิตที่ติดเชื้อกระบวนการบูต (MBR, บูตเซกเตอร์ หรือเฟิร์มแวร์ UEFI) จึงทำงานก่อนที่ระบบปฏิบัติการจะโหลด

Q8: การสแกนแบบฮิวริสติกระบุภัยคุกคามซีโร่เดย์ได้อย่างไร?

สแกนรูปแบบโค้ดที่น่าสงสัยและคำสั่งผู้ดูแลระบบ แทนการมองหาแฮชในฐานข้อมูลที่ตรงกัน

Q9: ภัยคุกคามจาก DLL hijacking คืออะไร?

การบังคับให้แอปพลิเคชันที่ถูกต้องโหลดไลบรารีลิงก์ไดนามิก (DLL) ที่เป็นอันตรายโดยวางไว้ในเส้นทางไดเรกทอรีของแอปพลิเคชัน

Q10: ไปป์ไลน์วิเคราะห์มัลแวร์อัตโนมัติใช้เวอร์ชวลไลเซชันอย่างไร?

รันไฟล์น่าสงสัยบน VM ของหลาย OS และสร้างบันทึกพฤติกรรมกับไฟล์ PCAP ของเครือข่ายโดยอัตโนมัติ

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

โทรจันยังเป็นวิธีติดเชื้อที่พบบ่อย เพราะซ่อนโค้ดอันตรายไว้ในโปรแกรมที่ดูไม่มีพิษภัย

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

IC3 ของ FBI ได้รับเรื่องร้องเรียนแรนซัมแวร์กว่า 3,600 รายการในปี 2025 โดยมีรายงานความเสียหายเกิน 32 ล้านดอลลาร์ [3]

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

เวิร์มสามารถแพร่กระจายข้ามเครือข่ายได้อย่างรวดเร็วโดยใช้ช่องโหว่ของโปรโตคอลที่ยังไม่ได้แพตช์ เช่น EternalBlue ใน SMB

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

มัลแวร์ไร้ไฟล์ตรวจจับได้ยากเพราะรันในหน่วยความจำผ่านเครื่องมือที่ถูกต้องและทิ้งร่องรอยบนดิสก์เพียงเล็กน้อย

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

แซนด์บอกซ์สำหรับการวิเคราะห์มักย้อนกลับไปยังสแนปช็อตที่สะอาดหลังการรันแต่ละครั้ง เพื่อให้ทุกการทดสอบเริ่มจากสถานะที่ทราบ

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

รูทคิตสามารถแก้ไขการเรียกระบบของเคอร์เนล ทำให้รายงานผลวินิจฉัยเท็จแก่ตัวสแกนมัลแวร์

7. ข้อมูลเชิงลึกด้านความปลอดภัย

การอำพรางโค้ดใช้ยูทิลิตีแพ็กเกอร์เพื่อบีบอัดและซ่อนโครงสร้างเพย์โหลดไบนารีที่แท้จริงของมัลแวร์

8. ข้อมูลเชิงลึกด้านความปลอดภัย

มัลแวร์โพลีมอร์ฟิกเปลี่ยนโค้ด และเปลี่ยนแฮชของไฟล์ไปด้วย ในแต่ละสำเนาใหม่เพื่อหลบการตรวจสอบลายเซ็น

9. ข้อมูลเชิงลึกด้านความปลอดภัย

DLL hijacking ใช้ประโยชน์จากการกำหนดค่าลำดับการค้นหาในระบบปฏิบัติการทั่วไป เช่น Windows

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ผู้จำหน่ายด้านความปลอดภัยพบตัวอย่างมัลแวร์ใหม่จำนวนมหาศาลทุกวัน ลายเซ็นจึงต้องได้รับการอัปเดตอย่างต่อเนื่อง

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ลักษณะเฉพาะที่กำหนดม้าโทรจันคืออะไร? → ปลอมตัวเป็นซอฟต์แวร์ที่ถูกต้องเพื่อหลอกให้ผู้ใช้รัน

2 คำถาม 2 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

มัลแวร์ประเภทใดที่เข้ารหัสไฟล์และเรียกเก็บเงิน? → แรนซัมแวร์

3 คำถาม 3 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

อะไรแสดงถึงสปายแวร์? → มัลแวร์ที่ออกแบบมาเพื่อแอบตรวจสอบการกดแป้นพิมพ์และกิจกรรมเบราว์เซอร์ของผู้ใช้

4 คำถาม 4 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

เหตุใดนักพัฒนามัลแวร์จึงใช้รูทคิท? → เพื่อซ่อนโพรเซสที่ทำงานอยู่และไฟล์อันตรายจากระบบปฏิบัติการ

5 คำถาม 5 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

แซนด์บ็อกซ์หมายถึงอะไรในการวิเคราะห์มัลแวร์? → การรันไฟล์น่าสงสัยในห้องนิรภัยเสมือนที่แยกต่างหากเพื่อสังเกตพฤติกรรมอย่างปลอดภัย

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: เวิร์มแพร่พันธุ์ตัวเองและแพร่กระจายผ่านเครือข่ายโดยที่ผู้ใช้ไม่ต้องทำอะไร

7 **คำถาม 7** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: แอดแวร์ไม่ได้ไม่เป็นอันตรายเสมอไป แอดแวร์จำนวนมากติดตามการเรียกดูเพื่อกำหนดเป้าหมายโฆษณา

8 **คำถาม 8** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: ข้อมูลสำรองออฟไลน์ที่สะอาดกู้ไฟล์ที่ถูกเข้ารหัสได้โดยไม่ต้องจ่ายเงิน แม้ข้อมูลที่ถูกขโมยอาจยังรั่วไหลได้

9 **คำถาม 9** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: ตัวสแกนแบบซิกเนเจอร์ต้องมีตัวอย่างที่ทราบ มัลแวร์ zero-day ใหม่เอี่ยมจึงอาจหลุดรอดไปได้

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

มัลแวร์ไร้ไฟล์รันสคริปต์อันตรายในหน่วยความจำของระบบ หลีกเลี่ยงการเขียนไฟล์ลงดิสก์

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

D 1. โทรจัน	F 2. แรนซัมแวร์	A 3. สปายแวร์	H 4. รูทคิต
G 5. แซนด์บ็อกซ์	C 6. การจำกัดขอบเขต	E 7. เวิร์ม	B 8. ไร้ไฟล์

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 โทรจัน	2 แรนซัมแวร์	3 สปายแวร์	4 รูทคิต
5 แซนด์บ็อกซ์	6 กักกัน		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 D – รูทคิต	2 F – กักกัน	3 H – ไร้ไฟล์	4 G – เวิร์ม
5 B – แรนซัมแวร์	6 C – สปายแวร์	7 A – โทรจัน	8 E – แซนด์บ็อกซ์

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย โทรจัน แรนซัมแวร์ และ สปายแวร์ ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

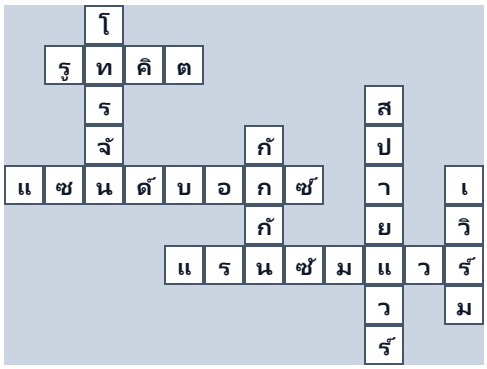
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ก	ก	ก	ต	ด	ค	ก	ผ	น	า	า	รู	า	ก	ด
ส	ก	ส	ต	า	า	ต	พ	ส	จั	ส	า	ท	น	ว
บ	ต	ส	ว	จ	ท	ล	ท	ด	า	ร	ก	ต	ค	ท
า	า	า	ร	อ	ส	ฟ	ก	า	ร	ส	ท	พ	น	ต
ส	า	ก	ผ	ส	ช	ล์	บ	ร	ฟ	ต	ด	โ	า	ด
แ	ต	เ	า	พ	ฟ	า	ค	า	ม	ช	ร	ส	ว	ว
ร	ต	า	ว	ไ	บ	บ	ส	ด	ย	า	ช	ด	ก	ห
น	ม	ฟ	ร้	ร์	น	ม	ง	ด	ร	ส	ช	ม	ก	า
ช้	า	ไ	ส	ต	ม	ม	ส	ป	า	ย	แ	ว	ร์	ค
ม	ผ	ช์	ก	อ	บ	ด์	น	ช	แ	บ	ต	ม	ก	ท
แ	ช	ผ	ง	ต	ย	า	ก	พ	ว	ห	ท	ร	ท	ร
ว	ต	า	ค	น	น	ก้	ต	า	น	ต	ต	ข	ท	ก
ร์	ผ	ด	า	ร	ก	ผ	ง	ด	ส	ว	ก	ง	ง	ห
ส	ด	ร	ต	ก้	า	ม	ส	ส	า	ต	พ	ร	า	า
น	า	พ	น	ล	ล	ม	า	ป	น	ม	า	ข	ด	ฟ

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: รูทคิต มัลแวร์แฝงตัวลึกในเคอร์เนลของระบบเพื่อรักษาการควบคุมระดับผู้ดูแลไว้ (4 ตัวอักษร)

5 แนวนอน: แซนด์บอกซ์ สภาพแวดล้อมเสมือนที่แยกขาดซึ่งใช้วิเคราะห์ไฟล์อันตรายอย่างปลอดภัย (8 ตัวอักษร)

7 แนวนอน: แรนซัมแวร์ มัลแวร์ที่เข้ารหัสพื้นที่จัดเก็บของระบบและเรียกค่าไถ่เพื่อส่งมอบกุญแจ (8 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: โทรจัน ซอฟต์แวร์ประสงค์ร้ายที่ปลอมตัวเป็นโปรแกรมอรรถประโยชน์ที่ไม่เป็นอันตรายหรือมีประโยชน์ (5 ตัวอักษร)

3 แนวตั้ง: สปายแวร์ โปรแกรมที่ออกแบบมาเพื่อแอบเฝ้าดูและบันทึกกิจกรรมและข้อมูลที่ผู้ใช้ป้อน (7 ตัวอักษร)

4 แนวตั้ง: กักกัน การจำกัดอุปกรณ์ปลายทางที่ติดเชื้อเพื่อป้องกันการแพร่ของเพย์โหลดภัยคุกคาม (4 ตัวอักษร)

6 แนวตั้ง: เวิร์ม มัลแวร์ที่ทำสำเนาตัวเองและแพร่ผ่านเครือข่ายโดยไม่ต้องมีการกระทำของมนุษย์ (4 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. จ์รโนท — **โทรจัน**
2. สาร์วแยป — **สปายแวร์**
3. ด์ซแบอซ์กน — **แซนด์บอกซ์**
4. มร์เว — **เวิร์ม**
5. มแรร์ซ์แวน — **แรนซัมแวร์**
6. คิตรูท — **รูทคิต**
7. กักันก — **กักกัน**
8. ส์ไฟร้ — **ไร้ไฟส์**

เฉลยภารกิจรหัสลับ

"ตรวจจับ เพย์โหลด ปลายทาง ด้วย ตัวเฝ้าดู"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การจำกัดเพย์โหลดแรนซัมแวร์ในองค์กร

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: เครือข่ายท้องถิ่นขององค์กรถูกแรนซัมแวร์ที่กำลังทำงานเจาะเข้ามา เซิร์ฟเวอร์ไฟล์หลักเริ่มแสดงนามสกุลไฟล์ .locked จงกำหนดนโยบายการจำกัดวงความเสียหาย
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ตัดการเชื่อมต่อเซิร์ฟเวอร์ที่ได้รับผลกระทบทั้งหมดออกจากเครือข่ายท้องถิ่น ยุติเซสชันผู้ดูแลระบบที่ใช้งานอยู่ กู้คืนไฟล์ที่ไม่ได้รับผลกระทบจากระบบสำรองข้อมูลออฟไลน์ที่ปลอดภัยและล็อกการเขียน

B กรณีศึกษาที่ 2: การฉีดหน่วยความจำของมัลแวร์ไร้ไฟล์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: นักวิเคราะห์ตรวจพบรูปแบบสคริปต์น่าสงสัยที่ทำงานโดยตรงใน RAM ชั่วคราวของระบบโดยใช้เครื่องมือผู้ดูแลระบบมาตรฐาน แต่ไม่มีไฟล์อันตรายบนดิสก์
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: แยกอุปกรณ์ปลายทางที่ได้รับผลกระทบและจับภาพหน่วยความจำก่อน ตรวจสอบบันทึก PowerShell และ WMI บล็อกสคริปต์ที่ไม่ได้รับอนุญาตด้วย AppLocker แล้วรีบูตเพื่อล้างเพย์โหลด